

**Обоснование невозможности закупки программ для ЭВМ, включенных
в Единый реестр российских программ для электронных
вычислительных машин и баз данных**

**по конкурсу в электронной форме на право заключения договора на
выполнение работ по созданию подсистемы управления событиями
информационной безопасности объектов критической информационной
инфраструктуры АО «СО ЕЭС», приобретение программного
обеспечения для АО «СО ЕЭС»
(далее - конкурс)**

Предметом конкурса является, в том числе:

1. Поставка экземпляров программ для ЭВМ производителя
(правообладателя) Rapid7:

NXRTECHSUB-RES	Экземпляр программы для ЭВМ Rapid7 RES Nexpose 15k Maint., Upgrades, Vulnerability subscription Additional Year
NXENTALLTERM-RES	Экземпляр программы для ЭВМ Rapid7 RES Nexpose Subscription 12months
NXENTALLTERM-RES	Экземпляр программы для ЭВМ Rapid7 RES Nexpose Subscription 13months

(далее совместно именуемые - Программы для ЭВМ Rapid7);

2. Поставка экземпляров программ для ЭВМ MFE производителя
(правообладателя) McAfee:

ACE2600ARMA A	Экземпляр программы для ЭВМ MFE Adv Corr Eng 2600 BZ+ARMA
ETMX4NBDA	Экземпляр программы для ЭВМ MFE Ent Sec Mgr X4 BZ+NBD

3. Предоставление права использования программ для ЭВМ MFE
производителя (правообладателя) McAfee:

ICGYCM-AD-AA	Право использования ПО MFE Network Sec Central Mgr Glbl 1YrBZ
IMGYCM-AD-AA	Право использования ПО MFE Network Sec Global Mngr 1Yr BZ
VC3ECE-AB-AA	Право использования ПО MFE vNSP Cloud Large (1Gbps) 1:1 BZ

VC3ECE-AB-AA	Право использования ПО MFE vNSP Cloud Large (1Gbps) 1:1 BZ
EV2VYE-AA-AA	Право использования ПО MFE Event Receiver VM 8 Cores 1 Yr BZ
EV2VYE-AA-AA	Право использования ПО MFE Event Receiver VM 8 Cores 1 Yr BZ
ENU4YE-AA-AA	Право использования ПО MFE Ent Sec Mngr VM 4 Cores Add-On BZ
ENUVYE-AA-AA	Право использования ПО MFE Ent Sec Manager VM 8 Cores 1 Yr BZ
EV2VYE-AA-AA	Право использования ПО MFE Event Receiver VM 8 Cores 1 Yr BZ
WSGYCM-AA- HA	Право использования ПО MFE Web Security 1Yr BZ
GAMECE-AA-HA	Право использования ПО MFE G/Way Anti Malware 1:1BZ

(далее совместно именуемые - Программы для ЭВМ MFE).

Закупаемые Программы для ЭВМ Rapid7 относятся к классам: средства анализа исходного кода на закладки и уязвимости, средства автоматизации процессов информационной безопасности.

Закупаемые Программы для ЭВМ MFE относятся к классам: средства обнаружения и/или предотвращения вторжений (атак), средства фильтрации негативного контента, средства управления событиями информационной безопасности, средства антивирусной защиты.

В АО «СО ЕЭС» эксплуатируется Комплексная система управления уязвимости (далее – КСУУ), обеспечивающая централизованное оперативное выявление и обработку уязвимостей информационных ресурсов в АО «СО ЕЭС», своевременное оповещение работников АО «СО ЕЭС», а также контроль установки обновлений.

В соответствии с Техно-рабочим проектом «Программно-аппаратный комплекс «Комплексная система управления уязвимостями», утвержденным директором по информационным технологиям АО «СО ЕЭС» 28.03.2018 (далее – ТРП), КСУУ построена на базе программно-аппаратного комплекса в составе оборудования со встроенным (предустановленным) программным обеспечением NEXPOSE ENTERPRISE производителя (правообладателя) Rapid7.

Закупаемые Программы для ЭВМ Rapid7 предназначены для расширения охвата одновременно инвентаризируемых (в части сканирования на наличие уязвимостей) ИТ-активов в АО «СО ЕЭС», являющихся подсистемой КСУУ.

Программы для ЭВМ MFE необходимы для обеспечения функционирования подсистем информационной безопасности, развернутых в АО «СО ЕЭС»: Единой Системы антивирусной защиты (далее - ЕСАЗ), Системы оперативного контроля информационной безопасности (далее - СОКИБ), Подсистемы обнаружения сетевых вторжений, являющейся подсистемой программно-аппаратного комплекса «Система защиты периметра корпоративной информационной системы АО «СО ЕЭС» (далее - ПОСВ).

Аналогичные программные средства российского производства, относящиеся к тем же классам: средства анализа исходного кода на закладки и уязвимости, средства автоматизации процессов информационной безопасности, средства обнаружения и/или предотвращения вторжений (атак), средства фильтрации негативного контента, средства управления событиями информационной безопасности, средства антивирусной защиты, включены в Единый реестр российских программ для электронных вычислительных машин и баз данных (далее – Реестр):

https://reestr.minsvyaz.ru/reestr/75106/?sphrase_id=213631

https://reestr.minsvyaz.ru/reestr/?sort_by=date&sort=asc&sort_by=date&sort=asc&name=&owner_status=&owner_name=&class=&class%5B%5D=54118&name=&owner_status=&owner_name=&set_filter=Y

Однако включенные в состав Реестра аналогичные программные средства российского производства **не соответствуют одновременно функциональным, техническим и эксплуатационным характеристикам** по сравнению с планируемыми к закупке Программами для ЭВМ Rapid7 и Программам для ЭВМ MFE (*основание: пункт 10 (б) статьи 7 Положения о порядке проведения регламентированных закупок товаров, работ, услуг для нужд акционерного общества «Системный оператор Единой энергетической системы» (шестая редакция)*), а именно:

– не обеспечивают полную совместимость с КСУУ, используемой в АО «СО ЕЭС», основанной на программном обеспечении Rapid7;

– не обеспечивают организацию своевременного контроля обработки уязвимостей в КСУУ;

– не обеспечивают возможность формирования отчетов совместимых с КСУУ;

- обеспечение функционирования следующих функциональных модулей СОКИБ, созданных на базе Программ для ЭВМ MFE, определенных в соответствии с утвержденным в АО «СО ЕЭС» Системно-техническим проектом на СОКИБ от 19.09.2016 № 631КТ:

- модуль сбора событий информационной безопасности (ИБ): должен иметь функциональную возможность активного сбора событий ИБ (сбор событий ИБ с использованием технологической

- учетной записи) и пассивного сбора событий ИБ (без доступа к источнику событий ИБ);
- модуль анализа событий ИБ: должен предоставлять возможность обработки не менее 180 000 событий в секунду);
 - модуль корреляции событий ИБ (должен иметь функциональную возможность анализа не менее 50 000 событий в секунду);
 - модуль хранения событий ИБ (должен иметь функциональную возможность сбора не менее 60 000 событий в секунду);
- обеспечение функционирования следующих функциональных модулей ЕСАЗ, созданных на базе Программ для ЭВМ МFE, определенных в соответствии с утвержденным в АО «СО ЕЭС» Системно-техническим проектом ЕСАЗ от 11.12.2019 № ИА-1252:
- средства антивирусной защиты на уровне шлюзов, обеспечивающих следующую функциональность:
 - Антивирусная фильтрация трафика;
 - Блокировка распространения вредоносного кода;
 - Помещение зараженных объектов в карантин;
 - Проксирование трафика;
 - Контентная фильтрация трафика;
 - Антиспам проверка почтового трафика.
 - средства централизованного управления и мониторинга компонентов антивирусной защиты, обеспечивающие централизованное управление для синхронизации политик между не менее 110 компонентами (шлюзами);
 - обеспечение функционирования следующих функциональных модулей ПОСВ, созданных на базе Программ для ЭВМ МFE, определенных в соответствии с утвержденным в АО «СО ЕЭС» Системно-техническим проектом СЗП от 19.12.2018 № ИА-1007КТ:
 - сенсоры обнаружения атак для сбора трафика, с предустановленным специализированным программным обеспечением для анализа трафика;
 - программное обеспечение управления сенсорами обнаружения, выполняющее роль сервера управления политиками.